

CLAIMS

What is claimed is:

- 1 1. A method of detecting a malware comprising the steps of:
 - 2 monitoring file access operations of a process;
 - 3 intercepting a file access operation of the process to a file;
 - 4 waiting a time interval; and
 - 5 scanning the file for a malware.
- 1 2. The method of claim 1, wherein the process is associated with an
2 application program.
- 1 3. The method of claim 1, wherein the file access operation is a file write
2 operation.
- 1 4. The method of claim 1, wherein the file has a specified file type.
- 1 5. The method of claim 1, wherein the time interval is predefined.
- 1 6. The method of claim 1, wherein the time interval is user-defined.

1 7. The method of claim 1, wherein the time interval is based on a filetype of
2 the file.

1 8. The method of claim 1, wherein the time interval is based on the process.

1 9. The method of claim 1, wherein the malware is a computer virus.

1 10. The method of claim 1, wherein the malware is a computer worm.

1 11. The method of claim 1, wherein the malware is a Trojan horse program.

1 12. The method of claim 1, further comprising the step of:
2 allowing the intercepted file access operation of the process to a file to
3 complete.

1 13. The method of claim 12, further comprising the step of:
2 allowing at least one additional file access operation of the process to a
3 file that occurs before the scanning of the file for a malware to complete.

1 14. A system for detecting a malware comprising:
2 a processor operable to execute computer program instructions;

3 a memory operable to store computer program instructions executable
4 by the processor; and
5 computer program instructions stored in the memory and executable to
6 perform the steps of:
7 monitoring file access operations of a process;
8 intercepting a file access operation of the process to a file;
9 waiting a time interval; and
10 scanning the file for a malware.

1 15. The system of claim 14, wherein the process is associated with an
2 application program.

1 16. The system of claim 14, wherein the file access operation is a file write
2 operation.

2 17. The system of claim 14, wherein the file has a specified file type.

1 18. The system of claim 14, wherein the time interval is predefined.

1 19. The system of claim 14, wherein the time interval is user-defined.

1 20. The system of claim 14, wherein the time interval is based on a filetype of
2 the file.

1 21. The system of claim 14, wherein the time interval is based on the process.

1 22. The system of claim 14, wherein the malware is a computer virus.

1 23. The system of claim 14, wherein the malware is a computer worm.

1 24. The system of claim 14, wherein the malware is a Trojan horse program.

1 25. The system of claim 14, further comprising the step of:
2 allowing the intercepted file access operation of the process to a file to
3 complete.

1 26. The method of claim 25, further comprising the step of:
2 allowing at least one additional file access operation of the process to a
3 file that occurs before the scanning of the file for a malware to complete.

1 27. A computer program product for detecting a malware comprising:
2 a computer readable medium;

3 computer program instructions, recorded on the computer readable
4 medium, executable by a processor, for performing the steps of
5 monitoring file access operations of a process;
6 intercepting a file access operation of the process to a file;
7 waiting a time interval; and
8 scanning the file for a malware.

1 28. The computer program product of claim 27, wherein the process is
2 associated with an application program.

1 29. The computer program product of claim 27, wherein the file access
2 operation is a file write operation.

1 30. The computer program product of claim 27, wherein the file has a
2 specified file type.

1 31. The computer program product of claim 27, wherein the time interval is
2 predefined.

1 32. The computer program product of claim 27, wherein the time interval is
2 user-defined.

1 33. The computer program product of claim 27, wherein the time interval is
2 based on a filetype of the file.

1 34. The computer program product of claim 27, wherein the time interval is
2 based on the process.

1 35. The computer program product of claim 27, wherein the malware is a
2 computer virus.

1 36. The computer program product of claim 27, wherein the malware is a
2 computer worm.

1 37. The computer program product of claim 27, wherein the malware is a
2 Trojan horse program.

1 38. The computer program product of claim 27, further comprising the step
2 of:

3 allowing the intercepted file access operation of the process to a file to
4 complete.

- 1 39. The computer program product of claim 38, further comprising the step
- 2 of:
- 3 allowing at least one additional file access operation of the process to a
- 4 file that occurs before the scanning of the file for a malware to complete.